10 WAYS TO SECURELY USE REMOVABLE MEDIA DEVICES

Bring your own device (**BYOD**) policies are adopted by organizations to allow better flexibility at work for employees but at the cost of opening gateways for USB-borne malware and unauthorized file transfers. It is therefore not surprising that the Ponemon Institute found that **67%** of IT professionals believe BYOD has lowered their level of security. However, there are workarounds to secure removable storage or peripheral devices to use them efficiently and with minimum risks. A few pointers for securely using removable media devices include the following:

1 Define a BYOD security policy

Draft and implement a policy to manage the use of USB drives and other removable media devices, focusing on rules to be followed and employees' accountability.

82% of companies actively enable BYOD.

2 Allow secure devices only

Authorize only the use of secure devices, like USB drives with fingerprint authentication or password protection.

37% of cybersecurity threats are targeted at removable media.

3 Password protect USB drives

Secure flash drives with passwords to render USB theft futile to insiders and ensure that the stolen data does not lead to a breach.

28% of cybersecurity attacks on endpoints in 2020 involved compromised or stolen devices.

4 Control user access

Use data leak prevention (DLP) software to control the level of access users can exercise. For instance, allow users to only read files within USB drives and block modification or application execution actions in USB drives.

51% of professionals feel that unauthorized access to data and systems is one of the top four threats.

5 Mandate data encryption

Require users to encrypt data stored or shared via removable storage devices to lower the consequences of theft or loss. Maintain multiple data backups, both in the cloud and offline.

56% of companies were able to retrieve data from backups rather than by paying ransom.

6 Block unauthorized USBs

Allow only USB devices accepted or recognized by the IT security team. Block other USB drives that may be bad USBs, plugged in by users, with a DLP solution.

22% of companies detected malware downloaded from unmanaged devices.

7 Audit file copy events

Track users who have copied sensitive files to immediately stall a potential breach. Block copy actions wherever necessary to prevent users attempting to transfer files to USB devices using copy prevention software.

45% of employees have admitted sharing work documents to personal accounts before leaving a job.

8 Maintain official USBs

Use organization-issued devices. Ensure that when devices are used again, they contain none of the previous files stored or shared.

82% of organizations cannot guarantee insider threat detection from employees' personal devices.

9 Authorize the right users

Review file permissions periodically and revoke excess privileges granted to users. Meticulously managing user privileges lowers the chances of an insider data leak or theft.

66% of insider threats led to privilege misuse to illegitimately access critical systems or data.

10 Protect against malware

Deploy antivirus and intrusion detection systems to ensure that unofficial devices aren't used by hackers or insiders to infiltrate the network.

32% of survey respondents were most concerned about the risk of malware infection.